Computers, Materials & Continua
DOI: 10.32604/cmc.2022.021519
Article

Tech Science Press

Image Encryption Using Multi-Scroll Attractor and Chaotic Logistic Map

R. Anitha* **and B. Vijayalakshmi**

Department of Electronics & Communication Engineering, B. S. Abdur Rahman Crescent Institute of Science & Technology, Chennai, 600045, Tamilnadu, India
*Corresponding Author: R. Anitha. Email: anitharajesh29@gmail.com
Received: 05 July 2021; Accepted: 24 December 2021

Abstract: In the current scenario, data transmission over the network is a challenging task as there is a need for protecting sensitive data. Traditional encryption schemes are less sensitive and less complex thus prone to attacks during transmission. It has been observed that an encryption scheme using chaotic theory is more promising due to its non-linear and unpredictable behavior. Hence, proposed a novel hybrid image encryption scheme with multi-scroll attractors and quantum chaos logistic maps (MSA-QCLM). The image data is classified as inter-bits and intra-bits which are permutated separately using multi scroll attractor & quantum logistic maps to generate random keys. To increase the encryption efficiency, a hybrid chaotic technique was performed. Experimentation is performed in a Qiskit simulation tool for various image sets. The simulation results and theoretical analysis show that the proposed method is more efficient than its classical counterpart, and its security is verified by the statistical analysis, keys sensitivity, and keyspace analysis. The Number of changing pixel rate (NPCR) & the Unified averaged changed intensity (UACI) values were observed to be 99.6% & 33.4% respectively. Also, entropy oscillates from 7.9 to 7.901 for the different tested encrypted images. The proposed algorithm can resist brute force attacks well, owing to the values of information entropy near the theoretical value of 8. The proposed algorithm has also passed the NIST test (Frequency Monobit test, Run test and DFT test).

Keywords: Chiper key; image encryption; logistic map; quantum chaos; qiskit

1 Introduction

The growth in digital communication and information technology fields creates a high requirement for data generation, transmission and storage. Medical images are highly sensitive data and need to be protected while transmitting [1–3]. Digital images exhibit more detailed information as a shared correlation among nearby pixels. Encryption of digital images is highly challenging and it does not suit the traditional Advanced Encryption Standard (AES) and Data Encryption Standard (DES) encryption algorithm. Chaotic encryption schemes are preferable because of their randomness property in a key generation [4–7].

The existing chaos-based encryption model needs more improvisation to withstand vulnerable cyber-attacks including botnet, Denial of Service (DoS) and Man in the Middle (MITM) attacks [7]. The requirement of an efficient chaos scheme must expel high randomness and complex key generation. The dynamic complex nature of the data introduces more possibilities for introducing chaotic models. Though the data are non-dynamic, complex encryption is required to withstand the security requirements [8,9]. The encryption algorithm thus needs a complex chaotic key generation system to withstand malicious encoding of protected data [10].

Quantum-based chaos encryption models are preferred for their complexity behavior. Quantum computing in image processing applications is introduced to perform classical image processing problems with quantum mechanics techniques. This invasion enhances the efficiency in the field of imaging and excels with its parallel processing skills. The images are represented as quantum bits say qubits are encoded to perform a specific task. The quantum encoding process requires $[(2*n) + 1]$ qubits to encode a raw image. The main goal of the quantum image encryption scheme is to preserve the original content of the input image bits that are encoded. The permutation of bits in the image by changing their coordinates can result in image encryption. Quantum encryption exhibits classical state behavior and they are highly sensible for dynamic behaviors in any system. Many types of research propagate the advantage of quantum-based chaotic encryption [11–14].

From the above observations, a novel encryption scheme with multi-scroll attractor and quantum chaotic logistic maps is proposed for data encryption. The various stages of novel MSA-QCLM include,

1) Chaotic key generation using multi-scroll attractor model and quantum logistic Maps.
2) The newly encrypted data is permutated with the initial condition of logistic maps.
3) New encrypted data by diffusion process ready for transmission.

The paper discussion starts with a literature Survey followed by the proposed MSA-QCLM algorithm. Experimentation setup results with comparative analysis were discussed and concluded with the future scope.

2 Literature Review

Ranjeet et al. [15] developed a method of security system for the transmission of computerized imaging. They used a quantum confusion map to encrypt the staggered picture data. The image data is quad-tree divided and each part is encrypted separately to produce a non-shrinkable new structure for transmission. The encryption is based on the frequency of the corresponding blocks. The shuffling of pixels in each block constitutes to new measurement matrix which acts as the random key. The model is sensitive to edge-based pixel values of each block of the image.

Zakariya et al. [16] developed an image encryption model for computerized signature transmission using quantum cryptographic schemes. The input is divided into quantum gates for the encryption process. The quantum gates are used to solve both classical and quantum issues. The data is encrypted, decrypted, matched and transmitted to three output parties. Quantum entry-based keys are generated and checked for tampering in the pathways. In the receiving end, the unscrambled data is retrieved with the quantum key received at the end. The model is tested using MATLAB using the Quad Quantum library. The communication established is slower due to the complex process.

Guodong [17] developed an image encryption model that depends on confusing guideline entropy. This includes the various parameters for a confused guide such as change, regulation and dissemination. The keys are generated in regard concerning the pixel position. Thus, the change of position

is communicated and resolved to upgrade the security. Even a slight change in plain data generates a significant difference in encryption. This shows highly excelled encryption in the majority of instances. The pixel distribution is limited beforehand of diffusion operation.

Xingbin et al. [18] proposed an encryption scheme that develops the encryption circuit based on bit logic. The inter-bit and intra-bit are arranged and disordered to calculate q-bit using XOR logic. These q-bit planes constitute the generation of chipper text. There will create a uniform change in pixel position. This encryption scheme withstands brute-force attacks. The key generated thus by pixel detangling shows more proficient security.

Jian et al. [19] developed an encryption scheme based on generating confused guide maps. It also uses the Lorenz tumultuous guide map for DNA coding. The image is recreated based on the generated maps. Histogram, correlation and entropy are evaluated. Though the input image has ups and downs, the encrypted image is relatively uniform thus withstanding statistical attacks. The encryption scheme is often unstable in highly dynamic environments.

Xing et al. [20] developed encryption based on the Region of Interest (ROI) principle. The image is partitioned into ROI and encrypted. This is introduced in real-time Internet of Things (IoT) gadgets and observed that the power consumption for establishing the disordered encryption is high. Lia et al. [21] made a detailed idea of chip-based cryptography. The features in the images constitute the structure and encryption key requirements for chip generation. They also summarized the attacks prone in communication at various levels. They highlighted the chosen plain text attack and its need for consideration to build strong encryption schemes.

Motivated from these papers and proposed the novel hybrid encryption algorithm to ensure the better security against the different statistical attacks.

3 Proposed MSA-QCLM Method

The proposed algorithm based on multi-scroll attractor and quantum logistic maps create a strong encryption scheme with multiple key generations at an intermediate level. The input image is divided into inter-bits and intra-bits & permuted based on the fractal scroll and logistic maps to generate a random encryption key. These keys are combined with the original image information to create a highly sensitive chiper key for efficient encryption.

3.1 Multi-Scroll Attractor Model

Dynamical systems with multi-scroll are more complex dynamics than chaotic systems with mono-scroll attractors. The state-space equation for automatic chaotic system is given by,

$$\dot{x}_1 = -ax_1 + bx_2x_3 \tag{1}$$

$$\dot{x}_2 = -cx_2^3 + dx_1x_3 \tag{2}$$

$$\dot{x}_3 = ex_3 - fx_1x_2 \tag{3}$$

The above Eqs. (1)–(3) can be adapted using hyperbolic function and modified in Eq. (6).

Eqs. (4) and (5) are similar to Eqs. (1) and (2).

$$\dot{x}_1 = -ax_1 + bx_2x_3 \tag{4}$$

$$\dot{x}_2 = -cx_2^3 + dx_1x_3 \tag{5}$$

$$\dot{x}_3 = ex_3 - fx_1x_2 + p_1 tanh(x_2 + h) \tag{6}$$

Chaotic attractor is obtained when $a = 2, b = 6, c = 6, d = 3, e = 3, f = 1, p_1 = 1, h = 2$ and the preferred initial conditions include $(x_1[0], x_2([0], x_3[0]) = (0.1, 0.1, 0.6)$. Once the hyperbolic function is activated with the parameter, $h = -3$ and for the initial conditions generated, Fig. 1 illustrates various conditions of hyperbolic function. The second phase is initiated with the parameters $p_1 = -1, h = 3$ with the newly defined initial conditions as $[0.1, -0.1, -0.6]$. Fig. 2 illustrates the function regarding the new initial condition values. In the third phase, the parameters $p_1 = 1, h = 3$ and initial conditions are similar to the initially chosen values $[0.1, 0.1, 0.6]$. This is demonstrated in Fig. 3 which shows a single scroll. From the models, it is evident that the scheme is multi-scroll property.

To perform fractional estimates of chaotic systems, Eqs. (4) to (6) are adapted with the first, second and third-order derivative functions represented by Eqs. (7) to (9).

The newly derived models include,

$$\frac{d^q x_1}{dt^q} = -ax_1 + bx_2x_3 \tag{7}$$

$$\frac{d^q x_2}{dt^q} = -cx_2^3 + dx_1x_3 \tag{8}$$

$$\frac{d^q x_3}{dt^q} = ex_3 - fx_1x_2 + p_1 tanh(x_2 + g) \tag{9}$$

The bifurcation diagrams of the proposed multi-scroll system is shown in the following Fig. 4.

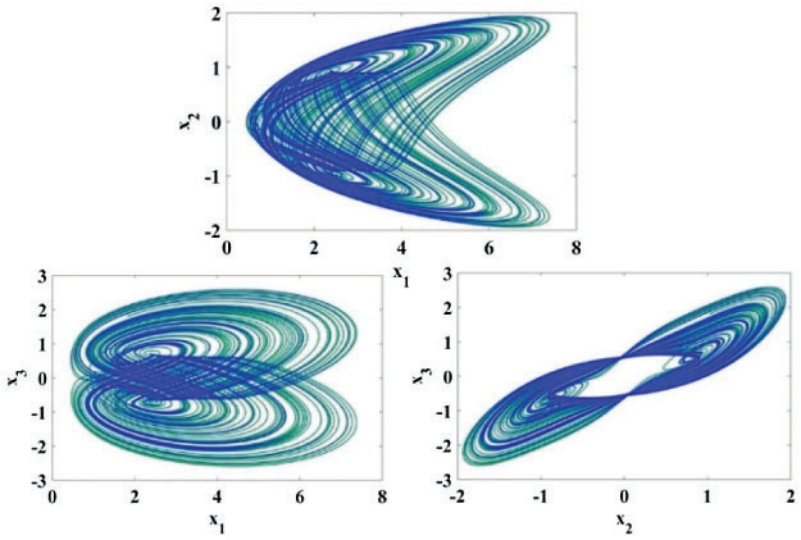

Figure 1: Portraits of phase for cubic nonlinear models of $p_1 \tanh(x_2 + h)$ function in 1st phase

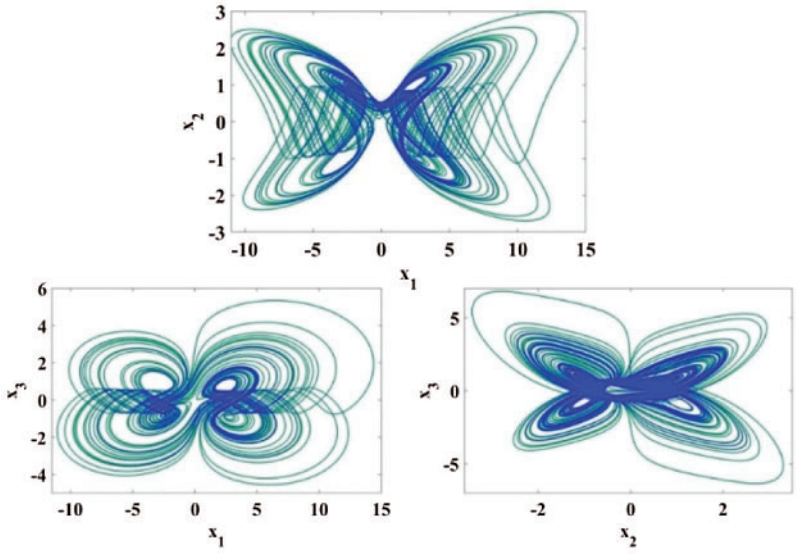

Figure 2: Portraits of phase for cubic nonlinear models of $p_1 \tanh(x_2 + h)$ function in 2nd phase

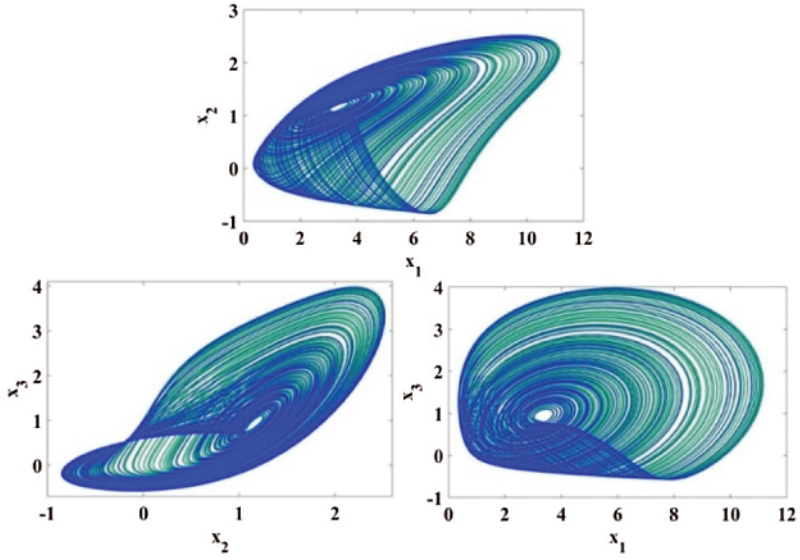

Figure 3: Portraits of phase for cubic nonlinear models of $p_1 \tanh(x_2 + h)$ function in 3rd phase

3.2 Logistic Maps

Chaotic systems are highly sensitive and are unpredictable in nature. The logistic maps are generated initially with basic permutation parameters. The bifurcation parameter varies from 0 to 4 when the iteration proceeds. The quantum logistic chaos maps are mainly generated with highly random outcomes.

The chaotic logistic maps are expressed as,

$$x_{m+1} = \mu x_m (1 - x_m) \tag{10}$$

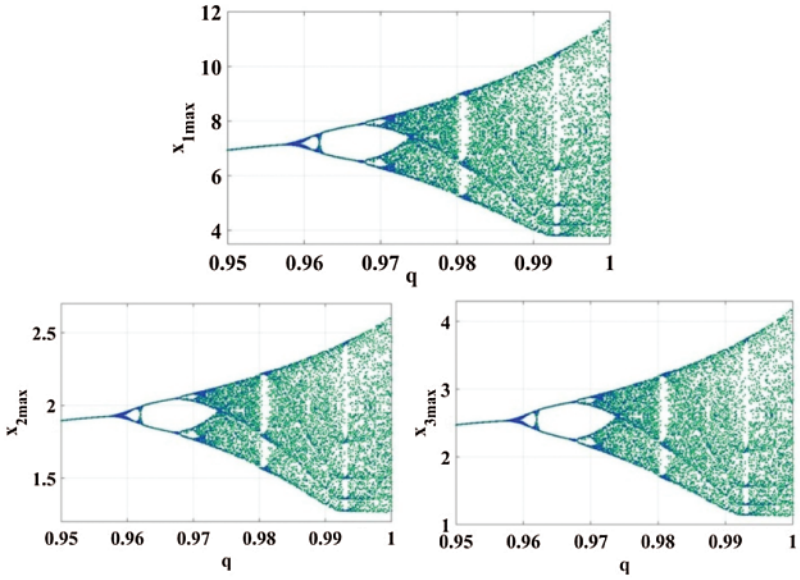

Figure 4: Bifurcation diagram of the proposed chaotic system

where, μ is the bifurcation parameter of logistic maps, with range $0 \leq \mu \leq 4$. The initial condition is chosen as $x_0 \in (0, 1)$ and as the iteration continues for 'm' numbers of sequences the threshold $3.5699456 < \mu \leq 4$ defines the chaotic nature of the system. As Kulsoom et al. [14] proposed the quantum logic maps is expressed as,

$$\left\{\begin{array}{c} a_{m+1} = C * (a_m - |a_m|) - C * f_m \\ b_{m+1} = -f_m * h^{-2\alpha} + h^{-\alpha} C\,[(2 - 2a_m) f_m - 2a_m d_m] \\ e_{m+1} = -d_m * h^{-2\alpha} + h^{-2\alpha} C\,[2(1 - a_m) d_m - 2a_m f_m - a_m] \end{array}\right\} \tag{11}$$

where, C denotes the control parameter, α is the dissipation constant, a_m & d_m are complex conjugate coordinates. Thus, the model is highly sensible such that a small change in data generates different pseudo-random sequences. As the iteration proceeds, the model exhibits the non-linearity required for medical image encryption.

3.3 Proposed MSA-QCLM Encryption Process

The complete encryption scheme using the proposed hybrid algorithm is given as a model in Fig. 5.

The encryption process is described as follows,

1. The Input Medical Images (grayscale images) are sub-divided into the inter-bit (pixels) I (m) and I(b) intra-bit (pixels) and rearranged into two M × N matrics
2. The intermediate keys are generated using the multi-scroll attractors using the Eqs. (4)–(6) which are denoted by the matrix S(m).
3. The matrix S(m) and I(m) are then diffused and permutated to form the new intermediate key K1 using the diffusion process given by,

$$\beta(1) = mod\ 256\ \{\sum I(m)\} \tag{12}$$

$$\mu(1) = F_i + \beta(1) + mod\ 256\ \{I(m)\} \tag{13}$$

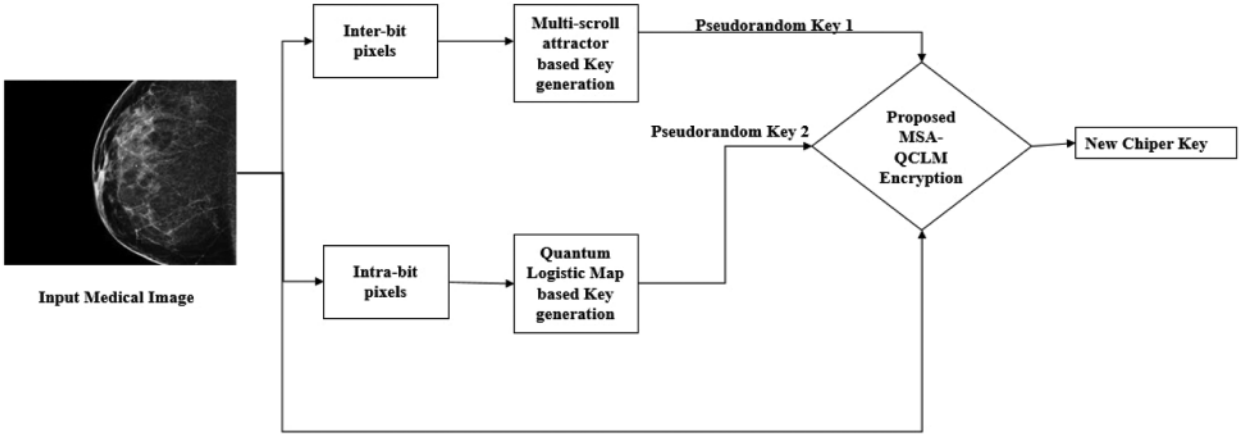

Figure 5: Proposed MSA-QCLM encryption process

Again,

$$\beta(2) = mod\ 256\ \{\sum S(m)\} \tag{14}$$

$$\mu(2) = F_i + \beta(2) + mod\ 256\ \{S(m)\} \tag{15}$$

$$\text{Total First key} = \text{K1} = \beta(1)\ permutated\beta(2) \tag{16}$$

4. The intermediate keys are generated using the 3D logistic maps using the Eqs. (7)–(9) which are denoted by the matrix Sl.
5. The matrix S(l) and I(b) are then diffused and permutated to form the new intermediate key K2 using the diffusion process given by,

$$\beta(3) = mod\ 256\ \{\sum I(b)\} \tag{17}$$

$$\mu(1) = F_i + \beta(3) + mod\ 256\ \{I(b)\} \tag{18}$$

Again,

$$\beta(4) = mod\ 256\ \{\sum S(l)\} \tag{19}$$

$$\mu(4) = F_i + \beta(4) + mod\ 256\ \{S(l)\} \tag{20}$$

$$\text{Total Second key} = \text{K1} = \beta(3)\ permutated\beta(4) \tag{21}$$

6. The total random key is generated by adding the Eqs. (16) and (21) which is given as the K matrix.

7. Again, the input image and newly formed key K is diffused to form the new encrypted images, the corresponding quantum circuit is given in Fig. 6

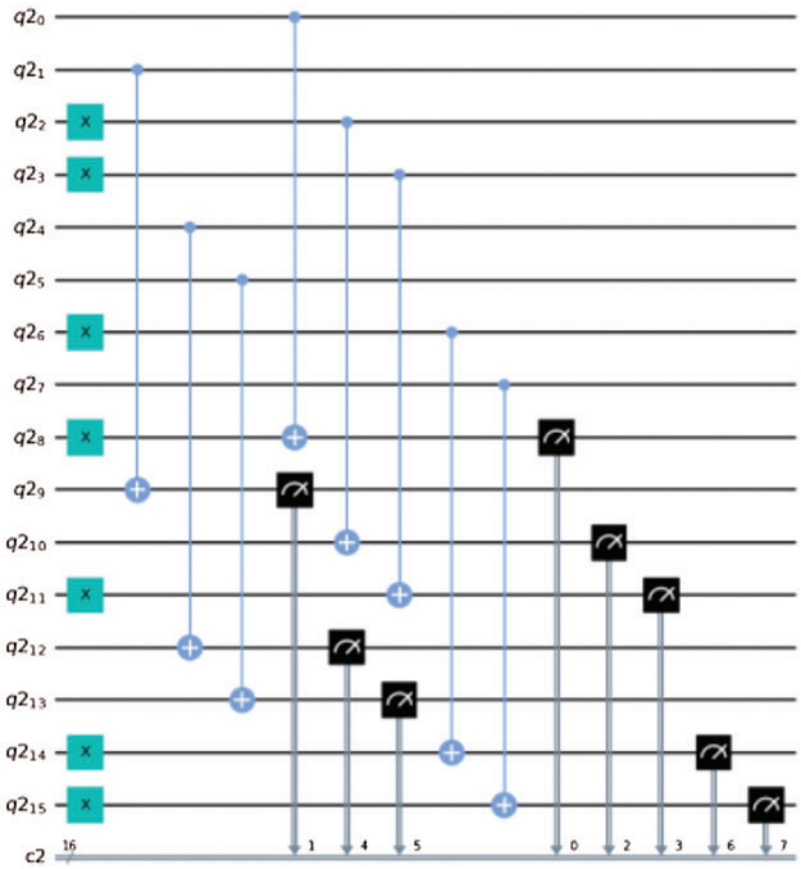

Figure 6: Quantum circuits for the implementation of proposed encryption

4 Results and Discussion

The performance of the proposed MSA-QCLM system is evaluated for the algorithm capability and the security ensured.

4.1 Performance of Security Analysis

The security assured by the proposed hybrid system is tested in distinct image sets. The general image set including Lena, Pepper, Baboon and medical data from the Mammogram Image Analysis Society (MIAS) model is utilized for experimentation. The image is chosen with a size of 256×256, shown in Fig. 7. The encrypted outputs of images are shown in Fig. 8 that has the better susceptible to different attacks. The whole experimentation has been implemented on i5 CPU with 4GB RAM, 1TBHDD, 3.2 GHZ frequency and Qiskit with necessary libraries were used for the complete development of the proposed algorithm.

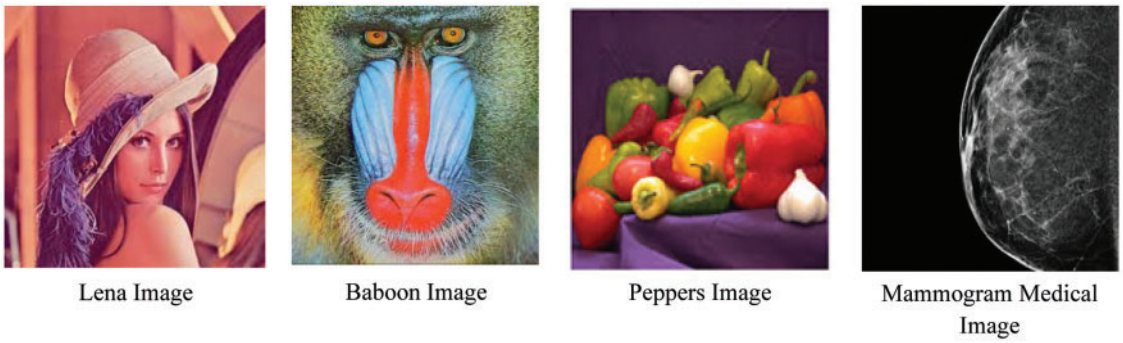

Figure 7: Input images

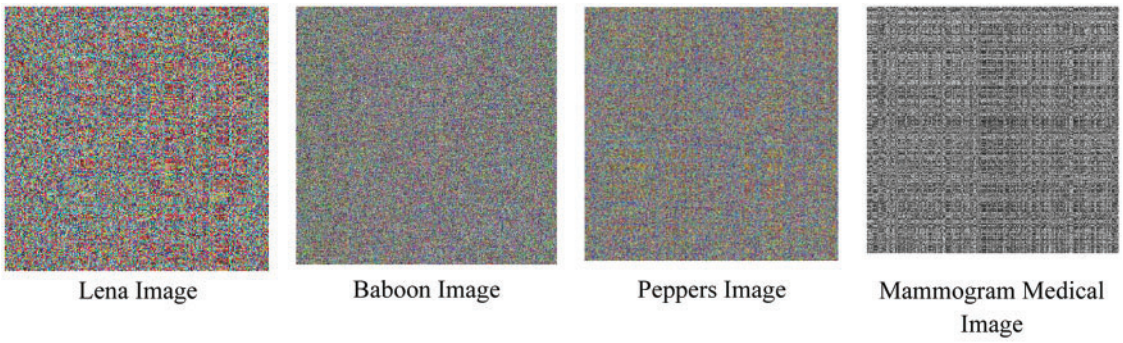

Figure 8: Encrypted output images

4.2 Key Sensitivity Analysis

It is of utmost importance to validate the sensitivity of key generated for its resistance towards mild to strong attacks. The number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) are the parameters used to test the performance of the encryption algorithm.

4.2.1 Randomness Test

NPCR focuses on the number of pixels that change due to attacks and UACI on the averaged difference between two paired ciphertext images. The NPCR & UACI metrics are calculated according to the Eqs. (22) and (23) to examine the proposed MSA-QCLM system. Tab. 1 shows the NPCR & UACI values for the input image set.

$$NPCR = \frac{\sum_{i,j} E(i,j)}{L} * 100 \tag{22}$$

$$\mathrm{U}ACI = \frac{1}{L}\sum_{i,j}\frac{|f(i,j) \neq f(i,j)|}{256} * 100 \tag{23}$$

where,

$$E(p,q) = \begin{bmatrix} 1, f(p,q) \neq f(p,q) \\ 0, f(p,q) = f(p,q) \end{bmatrix} \tag{24}$$

Table 1: NPCR & UACI analysis of four different input images

Image details	NPCR	UACI
Lena image	99.65%	33.56%
Pepper image	99.63%	32.54%
Baboon image	99.62%	33.45%
Mammogram image	99.65%	32.56%

The obtained results are compared with the other encryption algorithms and tabulated in Tab. 2. It gives the clear idea on strength of the proposed algorithm.

Table 2: Comparative analysis for other encryption schemes with respect to NPCR & UACI

Type of images	Sensitivity parameters	Ref. [17]	Ref. [19]	Proposed algorithm
Lena	NPCR	99.63%	99.56%	99.65%
	UACI	33.4%	28.54%	33.56%
Baboon	NPCR	99.56%	99.60%	99.62%
	UACI	33.38%	29.6%	33.45%

4.2.2 National Institute of Standards and Technology (NIST) Test

The strength of any encryption system will be highly related to the generated key. To ensure the key generated by the proposed algorithm is random, the paper employs the National Institute of Standards and Technology (NIST) procedural tests. The keys which are generated are converted into binary sequences and employed for the testing.

Frequency Monobit Test

The emphasis of the analysis is the ratio of one's and zero's throughout the whole series. The objective of this analysis is to decide whether the number of one's and zero's in a series is roughly the same as predicted. The measure evaluates the proximity of the percentage of one to 1/2, represents the number of one and zero in the series must be roughly the same. In this test, the zeros are assigned to -1 and the zeros are assigned to $+1$ and combined to generate the aggregate figures whose total mathematical formulation is presented as follows,

$$S = ||S(n)|| / n^{0.5} \tag{25}$$

where, 'S(n)' is the sum of the values attained and 'n' is the over-all sample count. Once the sum of values is calculated, the randomness is estimated by the 'P' value and is expressed as,

$$P = erfc(\frac{S}{2})^{0.5} \tag{26}$$

Run Test

The objective of this measure is to determine the cumulative number of cycles in a series even if the loop is a repeated series of the same pieces. The length 'k' run comprises precisely the same k bits and is connected pre and post with a bit of the contrary value. The objective of the training session is to decide if the number of tries of ones and zeroes of different lengths is as predicted in a random sequence. In specific, this measure decides if the oscillation among ones and zeros is too rapid or too sluggish.

This test uses a frequency test as a prerequisite. The key's continuity is examined for the randomness using the mathematical expression,

$$P = erfc(|V(n)(obs) - 2n\pi(1-\pi)|)/2.828n\pi(1-\pi) \tag{27}$$

where, V(n) (Obs) indicates the more rapid oscillations, when there is a lot of changes in the bitstreams.

DFT Test

The objective of this test seems to be the maximum height of the series in the Discrete Fourier Series. It identifies the recurrent characteristics (i.e., repeated structures that are close to one another) in the series which would imply a variation from the presumption of randomness. The complete test analysis of the key generated using the proposed hybrid chaotic applications are given in Tab. 3

Table 3: Complete test analysis

No of test details	Threshold to be obtained	Status of randomness
Frequency monobit test	$P > 0.01$	PASS
Run test	$P > 0.01$	PASS
DFT test	$P > 0.01$	PASS

Tab. 3 clearly shows the randomness of the keys is achieved by using the proposed hybrid algorithm and it has been proved that the generated key can defend any attacks in the networks for effective secured data transmission.

4.3 Adjacent Pixel Point Correlation Analysis

It is interesting to estimate the correlation factor of encrypted image and it has to be relatively low for an efficient encryption scheme. By comparing a set of 100 medical images, the correlation is estimated as follows,

$$R_{xy} = \frac{cov(a,b)}{\sqrt{E(x)E(y)}} \tag{28}$$

$$cov(a,b) = D\{[a - D(a)][b - D(b)]\} \tag{29}$$

$$e(a) = \frac{1}{n}\sum_{i=1}^{n} a_i \tag{30}$$

$$L(x) = \frac{1}{n}\sum_{i=1}^{n}[a_i - a(x)]^2 \tag{31}$$

where $e(a)$ and $L(x)$ indicates the expectations and variance of the normal image and encrypted images. Tab. 4 shows the correlation coefficient of the input and encrypted images. From the results, it is clear that the adjacent pixels are highly correlated in input but less correlation between the pixels in encrypted images.

Table 4: Correlation co-efficient of the input image and encrypted images

Image details	Raw images			Cipher images		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena images	0.89981901	0.8678909	0.456789	0.03032589	0.03032567	0.032891
Baboon images	0.9078920	0.967856	0.785436	0.0306792	0.034567	0.03391
Peppers images	0.89234	0.876590	0.56789	0.0308913	0.0380238	0.035789
Mammogram images	0.8967425	0.8854367	0.865783	0.0067890	0.005432	0.000185

4.4 Information Entropy Analysis

Entropy analyzes the randomness of information distribution in encrypted images**.** The higher entropy value relates to better irregularity in the encrypted images**.** Mathematically it is represented as,

$$g(m) = \sum_{l}^{l-1} q(m)\log_2\frac{1}{q(m_i)} \tag{32}$$

The values of entropy vary from 1 to 8. The different entropy values observed for various data sets are shown in Tab. 5.

Table 5: Entropy values for the various image samples

Sample datasets of encrypted image	Entropy values
Lena image	07.99
Baboon image	07.98
Peppers image	07.99
Mammogram image	07.99

Tab. 5 shows the various entropies of the various image sets that were observed to be nearly equal to 8.

4.5 Computational Time Complexity Analysis

A faster response rate is another requirement for any system to encrypt data. By injecting few attacks, the algorithm was tested for its response time. The input images with dimensions 256 × 256 are considered and assessed the time frame which is shown in Tab. 6

Table 6: Computational time complexity estimation

Sample dataset	Encryption time(s)
Lena image	0.567
Baboon image	0.567
Peppers image	0.566
Mammogram image	0.564

4.6 Diehard Randomness Test

To prove the randomness of the proposed encryption algorithm, we have conducted Diehard test which gives measurable indicators of randomness of cipher-text. The diehard battery includes twelve tests of which few are repeated with different parameters. As mentioned in [22], we conducted 12 test such as birthday test, overlapping test, permutations, binary rank, 3D-spheres, squeeze, overlapping sum, craps, minimum distance, parking lot, monkey test and runs. Tabs. 7 to 10 shows the different *p*-values of encrypted images. It is found from the Tabs. 7 to 10, *p*-values are found to be greater than 0.01 as mentioned in [23], which proves the proposed encryption can defend network and statistical attacks.

Table 7: Diehard randomness test for encrypted lena image

Test	*P*-value	Test	*P*-value
Birthday spacing	0.78748	Monkey test	0.87672
Overlapping	0.765738		0.90342
Permutations	0.75638		0.78920
Binary rank	0.8645		0.8562
Count the 1's	0.7652		0.7851
3D spheres	0.8657		0.7312
Squeeze	0.79300		0.8089
Overlapping sum	0.7867	Runs	0.7230
Craps	0.8645		0.73452
Min. distance	0.77790		0.67845
Parking lot	0.8902		0.92011

Table 8: Diehard randomness test for encrypted Baboon image

Test	*P*-value	Test	*P*-value
Birthday spacing	0.7882	Monkey test	0.7634
Overlapping	0.67892		0.6530
Permutations	0.7820		0.72302
Binary rank	0.73421		0.71011
Count the 1's	0.8021		0.80901
3D spheres	0.8532		0.78650
Squeeze	0.81201		0.8012
Overlapping sum	0.801	Runs	0.82101
Craps	0.78901		0.80178
Min. distance	0.7778		0.79067
Parking lot	0.88034		0.89012

Table 9: Diehard randomness test for encrypted peppers image

Test	*P*-value	Test	*P*-value
Birthday spacing	0.7673	Monkey test	0.8721
Overlapping	0.6867		0.8921
Permutations	0.5678		0.6210
Binary rank	0.8902		0.6732
Count the 1's	0.7421		0.8982
3D spheres	0.67891		0.9082
Squeeze	0.7812		0.9013
Overlapping sum	0.9021	Runs	0.8234
Craps	0.7003		0.7300
Min. distance	0.8920		0.8823
Parking lot	0.7341		0.88569

Table 10: Diehard randomness test for encrypted mammogram image

Test	*P*-value	Test	*P*-value
Birthday spacing	0.6634	Monkey test	0.6734
Overlapping	0.7834		0.7890
Permutations	0.7432		0.6732
Binary rank	0.892		0.85334
Count the 1's	0.9023		0.9012

(Continued)

Table 10: Continued

Test	*P*-value	Test	*P*-value
3D spheres	0.7820		0.7823
Squeeze	0.8021		0.8120
Overlapping sum	0.6789	Runs	0.8013
Craps	0.78230		0.6823
Min. distance	0.7320		0.6704
Parking lot	0.88235		0.8902

Tab. 11 shows the comparative analysis between the proposed algorithm and other state of art algorithms.

Table 11: Comparative analysis between proposed algorithm and other algorithm

Images	Algorithms	NPCR analysis	UACI analysis	Entropy	Computational time complexity
Encrypted lena image	Logistic maps	99.33%	33.21%	7.9992	Low
	Henon maps	99.45%	33.4%	7.8889	Low
	Multi-scroll attractors	99.55%	33.21%	7.9990	Low
	Proposed algorithm	99.65%	33.56%	7.9999	High
Encrypted baboon image	Logistic maps	99.24%	33.11%	7.9990	Low
	Henon maps	99.32%	33.2%	7.8888	Low
	Multi-scroll attractors	99.40%	33.19%	7.9991	Low
	Proposed algorithm	99.62%	33.45%	7.9898	High
Encrypted peppers image	Logistic maps	99.2%	33.19%	7.9991	Low
	Henon maps	99.30%	33.23%	7.8888	Low
	Multi-scroll attractors	99.29%	33.14%	7.9990	Low
	Proposed algorithm	99.63%	33.54%	7.9999	High
Encrypted mammogram image	Logistic maps	99.33%	31.21%	7.9992	Low
	Henon maps	99.32%	32.4%	7.8889	Low
	Multi-scroll attractors	99.50%	31.21%	7.9990	Low
	Proposed algorithm	99.65%	32.56%	7.9999	High

5 Conclusion

The proposed hybrid encryption algorithm enhances data security in dynamic environments. The proposed MSA-QLCM system is aware of the threats that occur during data transmission with a strong encryption key. The simulation results and theoretical analysis show that the proposed method is more efficient than its classical counterpart. The statistical analysis, keys sensitivity analysis, and key space analysis have been done. For the given medical data and standard images, the NPCR and UACI are found to be in the range of 99.8% and 33.5% respectively. Also, it has passed the NIST test and correlation values were very less after the encryption process. The entropy values oscillate between 7.9 to 8.0. Even though the proposed algorithm finds its applications in medical data transmission; the algorithm still requires profound improvement in terms of implementing the high intelligent algorithm. Future work can be extended to X dimensional hybrid chaotic system integrating the complex operations over the hybrid maps.

Acknowledgement: Thanks to the reviewing committee for their valuable points and notes.

Funding Statement: The author received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. Axenides, E. Floratos and S. Nicolas, "The quantum cat map on the modular discretization of extremal black hole horizons," *The European Physical Journal C*, vol. 78, pp. 1–15, 2018.

[2] A. Akhshani, A. Akhavan, A. Mobaraki, S. Lim and Z. Hassan, "Pseudo random number generator based on quantum chaotic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 1, pp. 101–111, 2014.

[3] E. Ahmed, A. Anees, V. Abbas and M. Siyal, "A noisy Channel tolerant image encryption scheme," *Wireless Personal Communication*, vol. 77, no. 4, pp. 2771–2791, 2014.

[4] A. Bakhshandeh and Z. Eslami, "An authenticated image encryption scheme based on chaotic maps and memory cellular automata," *Optics and Lasers in Engineering*, vol. 51, no. 6, pp. 665–673, 2013.

[5] A. Akhshani, A. Akhavan, S. Lim and Z. Hassan, "An image encryption scheme based on quantum logistic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 12, pp. 4653–4661, 2012.

[6] G. Ye and K. Wong, "An efficient chaotic image encryption algorithm based on a generalized Arnold map," *Nonlinear Dynamics*, vol. 69, no. 4, pp. 2079–2087, 2012.

[7] X. Ji, S. Bai, Y. Guo and H. Guo, "A new security solution to JPEG using hyper-chaotic system and modified zigzag scan coding," *Communications in Nonlinear Science and Numerical Simulation*, vol. 22, no. 1, pp. 321–333, 2015.

[8] Y. He, Y. Q. Zhang and X. Y. Wang, "A new image encryption algorithm based on two-dimensional spatiotemporal chaotic system," *Neural Computing and Applications*, vol. 32, pp. 247–260, 2020.

[9] A. Alghafis, N. Munir, M. Khan and I. Hussain, "An encryption scheme based on discrete quantum map and continuous chaotic system," *International Journal of Theoretical Physics*, vol. 59, pp. 1227–1240, 2020.

[10] Q. Zhang, L. Guo and X. Wei, "Image encryption using DNA addition combining with chaotic maps," *Mathematical and Computer Modeling*, vol. 52, no. 11–12, pp. 2028–2035, 2010.

[11] X. Y. Wang, Y. Q. Zhang and Y. Y. Zhao, "A novel image encryption scheme based on 2-D logistic map and DNA sequence operations," *Nonlinear Dynamics*, vol. 82, no. 3, pp. 1269–1280, 2015.

[12] X. Aqeelur Rehman, X. Liao, A. Kulsoom and S. Ullah, "A modified (Dual) fusion technique for image encryption using SHA-256 hash and multiple chaotic maps," *Multimedia Tools and Applications*, vol. 75, no. 18, pp. 11241–11266, 2016.

[13] A. Belazi, A. A. El-Latif and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.
[14] A. Kulsoom, D. Xiao, Aqeel-Ur-Rehman and S. A. Abbas, "An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules," *Multimedia Tools and Applications*, vol. 75, no. 1, pp. 1–23, 2016.
[15] S. Ranjeet Kumar Singh, K. Binod Kumar, W. Dilip Kumar Shaw and D. Danish Ali Khan, "Level by level image compression encryption algorithm based on Quantum chaos map," *Journal of King Saud University-Computer and Information Sciences*, vol. 33, no. 7, pp. 844–851, 2021.
[16] C. Zakariya Qawaqneh, M. Khaled Elleithy, A. Bandar Alotaibi and V. MunifAlotaibi, "A new hardware quantum-based encryption algorithm," in *IEEE Long Island Systems, Applications and Technology (LISAT) Conf. 2014*, Farmingdale, NY, pp. 1–5, 2014.
[17] R. Guodong Ye, "A chaotic image encryption algorithm based on information entropy," *International Journal of Bifurcation and Chaos*, vol. 28, no. 1, pp. 1850010, 2018.
[18] R. Xingbin Liu, W. Di Xiao and I. Yanping Xiang, "Quantum image encryption using intra and inter-bit permutation based on logistic map," *IEEE Access*, vol. 7, pp. 6937–6946, 2019.
[19] D. Jian Zhang and R. DaHuo, "Image encryption algorithm based on quantum chaotic map and DNA coding," *Multimedia Tools Applications*, vol. 78, pp. 15605–15621, 2019.
[20] E. Xing Zhang, W. Seung-Hyun Seo and A. Changda Wang, "A lightweight encryption method for privacy protection in surveillance videos," *IEEE Access*, vol. 6, pp. 18074–18087, 2018.
[21] C. Lia, Y. Zhang and E. Y. Xie, "When an attacker meets a cipher-image in 2018: A year in review," *Journal of Information Security and Applications*, vol. 48, 2019. https://doi.org/10.48550/arXiv.1903.11764.
[22] M. Mohammed Alani, "Testing randomness in cipher text of block-ciphers using diehard tests," *International Journal of Computer Science and Network Security*, vol. 10, no. 4, pp. 53–57, 2010.
[23] L. Sleem and R. Couturier, "Testu01 and practrand: Tools for a randomness evaluation for famous multimedia ciphers," *Multimedia Tools and Applications*, vol. 79, pp. 24075–24088, 2020.